Мр Милан Живановић

ПРИМЕНА ЈЕДНЕ ЛИНЕАРНЕ ТРАНСФОРМАЦИЈЕ КОД ВЕЛИКЕ ФЕРМАОВЕ ТЕОРЕМЕ

Нека је дата једначина

$$x^n + y^n = z^n, \qquad n \in \mathbf{N}. \tag{1}$$

Тврђење да једначина (1) нема решења у скупу природних бројева познато је као велика Фермаова теорема. Доказ тог тврђења публикован је у лето 1995. године од стране енглеског математичара Ендруа Вајлса.

Трансформацијом

$$x = \alpha + \gamma, \quad y = \beta + \gamma, \quad z = \alpha + \beta + \gamma \tag{2}$$

дата једначина постаје

$$(\alpha+\gamma)^n + (\beta+\gamma)^n = (\alpha+\beta+\gamma)^n,$$

$$\sum_{k=0}^{n} \binom{n}{k} \alpha^k \gamma^{n-k} + \sum_{k=0}^{n} \binom{n}{k} \beta^k \gamma^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (\alpha+\beta)^k \gamma^{n-k},$$

$$\sum_{k=0}^{n} \binom{n}{k} [\alpha^k + \beta^k - (\alpha+\beta)^k] \gamma^{n-k} = 0,$$

$$\sum_{k=0}^{n} \binom{n}{k} \left[-\sum_{l=1}^{k-1} \binom{k}{l} \alpha^{k-l} \beta^k \right] \gamma^{n-k} = 0,$$

$$\gamma^n - \sum_{k=2}^{n} \binom{n}{k} a_k \gamma^{n-k} = 0, \qquad a_k = \sum_{l=1}^{k-1} \binom{k}{l} \alpha^{k-l} \beta^l. \tag{3}$$

Означимо полином n-тог степена по променљивој γ на левој страни једначине (3) са $P_n(\gamma) = \gamma^n - \sum_{k=2}^{n} \binom{n}{k} a_k \gamma^{n-k}$. Он има неколико занимљивих особина. Прво, то је нормиран полином са целобројним коефицијентима код кога је коефицијент уз γ^{n-1} једнак 0. Друго, лако се проверава и једнакост $P'_n(\gamma) = nP_{n-1}(\gamma)$. И треће, ако је n прост број, тада су сви његови коефицијенти иза γ^n дељиви са $n\alpha\beta$.

Како су једначине (1) и (3) еквивалентне и с обзиром да је велика Фермаова теорема доказана, следи да ни једначина (3) нема решења у скупу природних бројева. Тврђење је могуће формулисати и на следећи начин.

Последица. *Нека су* $p, q \in \mathbf{N}$ *и нека је* $a_k = \sum\limits_{l=1}^{k-1} \binom{k}{l} \alpha^{k-l}\beta^l$. *Тада полином* $P_n(x) = x^n - \sum\limits_{k=2}^{n} \binom{n}{k} a_k x^{n-k}$ *нема целобројних нула.*

Прво решење Фермаовог проблема за случај $n = 3$ дао је Ојлер 1774. године. Тај доказ није био сасвим потпун, а недостаци у њему су отклоњени тек када је Лагранж објавио своје радове из квадратних бинарних форми. За $n = 5$ доказ Фермаове велике теореме су независно извели Лежандр и Дирихле, а за $n = 7$ Ламе. Најозбиљнији продор у доказивању општег случаја теореме дао је Кумер својом теоријом идеала. Очигледно је да је довољно доказати теорему за случај када је n просто. Радови који су се наставили на Кумерове ишли су у смеру побољшавања услова који важе за тај прост број n у Фермаовој једначини.

Дугогодишње истраживање проблема довело је до тога да практично можемо разликовати два основна случаја третирања проблема. Такозвани први случај велике Фермаове теореме важи уз услов $xyz \not\equiv 0 \pmod{n}$, и такозвани други случај је за $xyz \equiv 0 \pmod{n}$. Овде ћемо показати како се трансформацијом (2) за $n = 3$ први случај може елементарно доказати користећи Ајзенштајнов критеријум.

Ајзенштајнов критеријум. *Нека је дата једначина*

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0,$$

са коефицијентима из скупа целих бројева. Ако су сви коефицијенти $a_1, \ldots,$ a_{n-1} *дељиви простим бројем* p *и коефицијент* a_n *дељив са* p, *а није са* p^2, *тада дата једначина нема целобројних решења.*

Дакле, посматрајмо једначину

$$x^3 + y^3 = z^3 \tag{4}$$

и нека важи $xyz \not\equiv 0 \pmod 3$ и x, y, z су узајамно прости. Трансформацијом (2) она постаје

$$\gamma^3 - 6\alpha\beta\gamma - 3\alpha\beta(\alpha + \beta) = 0. \tag{5}$$

Из те једнакости следи да је $\gamma \equiv 0 \pmod 3$, но онда, како је $xy \not\equiv 0 \pmod 3$, закључујемо да је $\alpha\beta \not\equiv 0 \pmod 3$, а због $z \not\equiv 0 \pmod 3$ важи и $\alpha + \beta \not\equiv 0 \pmod 3$. Сада α и β дају исти остатак при дељењу са 3. Дакле, $\alpha \equiv \beta \equiv \pm 1 \pmod 3$, тј. $\alpha = 3k \pm 1$ и $\beta = 3l \pm 1$. Заменом овако записаних α и β у једначину (5) добијамо једначину

$$\gamma^3 - 6(3k \pm 1)(3l \pm 1)\gamma - 3(3k \pm 1)(3l \pm 1)(3k + 3l \pm 2) = 0$$

која према Ајзенштајновом критеријуму нема целобројних решења, јер су два последња коефицијента дељива са 3, а крајњи није са 9.

Занимљиво је да се коришћењем полинома $P_n(\gamma)$ могу добити неки комбинаторни идентитети.

Ако поделимо $P_n(\gamma)$ са $P_{n-1}(\gamma)$, добија се количник γ и остатак $R_n(\gamma) = -\sum\limits_{k=2}^{n}\binom{n-1}{k-1}a_k\gamma^{n-k}$. Тада је $P_n(\gamma) = \gamma\cdot P_{n-1}(\gamma) + R_n(\gamma)$. Вишеструком применом последње формуле имаћемо на крају

$$P_n(\gamma) = \gamma^n + R_2\gamma^{n-2} + R_3\gamma^{n-3} + \cdots + R_{n-1}\gamma + R_n.$$

Изједначавањем различито записаних израза за $P_n(\gamma)$ имамо да је:

$$\gamma^n - \sum_{k=2}^{n}\binom{n}{k}a_k\gamma^{n-k} = \gamma^n + \sum_{k=2}^{n}R_k(\gamma)\gamma^{n-k},$$

$$\gamma^n - \sum_{k=2}^{n}\binom{n}{k}a_k\gamma^{n-k} = \gamma^n + \sum_{k=2}^{n}\left(-\sum_{i=2}^{k}\binom{k-1}{i-1}a_i\gamma^{k-i}\right)\gamma^{n-k},$$

и најзад

$$\sum_{k=2}^{n}\binom{n}{k}a_k\gamma^{n-k} = \sum_{k=2}^{n}\left(\sum_{i=2}^{k}\binom{k-1}{i-1}a_i\gamma^{n-i}\right) = \sum_{k=2}^{n}\left(\sum_{i=k}^{n}\binom{i-1}{k-1}a_k\right)\gamma^{n-k}.$$

Као специјалан случај добија се и идентитет

$$\binom{n}{k} = \sum_{i=k}^{n}\binom{i-1}{k-1}.$$

Занимљиви идентитети се могу добити изједначавањем полинома $P_n(\gamma) = \gamma^n - \sum\limits_{k=2}^{n}\binom{n}{k}a_k\gamma^{n-k}$ и полинома $P_(\gamma) = (\alpha+\beta)^n + (\beta+\gamma)^n - (\alpha+\beta+\gamma)^n$ за једнаке вредности променљивих. Тако, на пример, за $\alpha=\beta=1$ и $\gamma=-1$ и n непарно имаћемо

$$-1 - \sum_{k=2}^{n}(-1)^{n-k}\binom{n}{k}(2^k-2) = -1, \quad \text{тј.} \quad \sum_{k=2}^{n}(-1)^{n-k}\binom{n}{k}(2^{k-1}-1) = 0.$$

У случају парности броја n, за исте вредности променљивих добија се једнакост $\sum\limits_{k=2}^{n}(-1)^{n-k}\binom{n}{k}(2^{k-1}-1) = 1$. Уврштавањем разних погодних вредности за α, β, γ могу се добити и други занимљиви бројевни идентитети.

Задаци за вежбање

1. За случај $n=4$ применити трансформацију (2) на једначину (1).

2. Извршити дељење $P_5(\gamma) : P_4(\gamma)$.

3. Без коришћења математичке индукције доказати идентитет
$$\binom{n}{k} = \sum_{i=1}^{n-k+1} i\binom{n-1-i}{k-2}.$$

4. Применом трансформације (2) доказати да једначина (1) за $n=5$ нема целобројних решења која су узајамно проста са 5.

ЛИТЕРАТУРА

1. В. Мићић, З. Каделбург, Д. Ђукић, ***Увод у теорију бројева***, 4. изд, Друштво математичара Србије, 2005.
2. М. Живановић, ***Инваријантна пресликавања Питагориних тројки***, Настава математике L, 1–2, ДМС, Београд, 2005.

Техничка школа, Бајина башта
E-mail: milanzibb@sezampro.yu